March 28, 1984

The Honorable William J. Hughes, Chairman
Subcommittee on Crime
Committee of the Judiciary
U. S. House of Representatives
2462 Rayburn House Office Building
Washington, D.C. 20515

Mr. Chairman. Members of the Subcommittee on Crime. My name is Wilbur C. Miller. I am the President of Drake University, which is located in Des Moines, Iowa. I am here today, by your invitation, to share my views on the "... future problems with electronic and computer fraud and the effect such innovations will have on educational institutions." At Drake, as with many institutions of higher education, this issue is not and has not been a consideration merely of problems for the future but has, in fact, been of great concern since the initial use of computers on the university campus. The views that I will be sharing with you are not hypothetical nor are they totally philosophical. On the evening of January 31, 1984, one of Drake University's computers was penetrated by hackers. These individuals had no connection with the University as students, faculty or staff and gained access to the computer through a telephone connection from an off-campus location. As a result of this unauthorized intrusion into the system, the University has been forced to dedicate scarce resources to the task of determining the extent and the effect of the intrusion. Many students and faculty members have been seriously inconvenienced

by having their research and curricular efforts restricted. While new and additional security provisions have been introduced following the intrusion, it must be understood that it is probably not possible to make an academic computing system totally secure against penetration by hackers. Use of the computer system in question goes on, but there is a new aura of concern. Users wonder, "Are my materials that I have stored in the computer system secure or have they been compromised?" Prudence dictates that the integrity of the system must be viewed as suspect and the use of the system for sensitive purposes must be curtailed. Indeed, this is the nature of the problem.

For those of you who may be unaware, Drake University is an independent comprehensive university. This fall, we enrolled in excess of 6,000 students. While the computing systems at Drake University are not as extensive as those at many large research universities, these systems are integral to carrying out the mission of the university. We have three central computer systems, a Digital Equipment Corporation VAX 11/780 dedicated to instruction and research; a Honeywell Level 64 DPS-320, dedicated to administrative processing activities such as maintenance of faculty, student and alumni data bases, and a Burroughs B800 on which many of the University's accounting and financial records are maintained. In addition to those which are owned by individual students and professors, the university has in excess of 50 personal computers. Current plans call for a

substantial increase in this number.

Drake University expenditures for computing represent approximately 2% of the annual budget. This level of spending is typical for comprehensive universities in the United States. According to Robert G. Gillespie, **Computing and Higher Education: an Accidental Revolution**, expenditures on computing in higher education were in excess of $1.3 billion in 1980. Since that time, higher education computing budgets have increased at a greater rate than overall expenditures.

Computer use by Drake faculty and students is heavy and growing. During the current year, instructional and research computer usage is three times greater than it was two years ago. This growth pattern is comparable to that experienced by other institutions of higher education. This year, 39% of our new freshman class indicated that they had written a computer program in the past year. This was an increase of nearly 10% over the previous class, and given the experiences that students are having with the estimated 325,000 computers now in the public school systems of the nation, this is a pattern that will continue.

In summary, computers have, in a very short period of time, become an essential element in the instructional, research and service missions of Drake University and of higher education in general. Investments in equipment and personnel are substantial

and the need to maintain secure systems is critical. What has in large part to date been viewed by the public as intellectual pranksterism on the part of computer hackers must be viewed as a serious intrusion on the rights of individuals to pursue the enterprise of their education in an accessible and reasonably secure academic environment.

It is a policy at Drake University that the use of computing facilities is as integral to the educational process as the use of library facilities. Therefore, computing facilities must be as readily accessible to faculty and students as those of the library. Accordingly, any currently enrolled student or member of the general faculty may use the academic computer for instructional or research purposes.

Minimal restrictions are placed upon the actions of computer users consistent with the effort to provide quality service to all users of the system. It is a mode of operation which relies upon the cooperation and trust of the participants. Few authorized computer users have taken advantage of this lack of restraints. However, when such advantage is taken, it can be readily recognized and for those who are charged with the responsibility of maintaining the system, the relative vulnerability of the system is reaffirmed. It is at this point that administrative action has been and must continue to be taken to enforce the prescribed standards of conduct for authorized users. We must also be willing to prosecute the criminal misuse

of our facilities. Legislation at both the state and federal levels is required to permit such criminal prosecution.

On the morning following the recent penetration incident, Drake Computer Center personnel were notified that the security of the academic computer system had been compromised by "hackers." In response, members of the computer center staff took a series of actions designed to identify the nature and seriousness of the intrusion, to guarantee that the system would be immune to additional intrusion attempts via the route taken by the "hackers," and to verify that the security mechanisms built into the computer by its manufacturer had not been altered or deactivated. Finally, provisions were made to gather more detailed data on the activities of each user of the system so that unauthorized use of the computer could be detected in a more timely manner.

These actions involved the participation of many computer center staff members and resulted in denial of access to the computer to students and faculty for over seven hours. The effect of these actions continued well beyond that day, however, since the computer resources required to monitor the detailed actions of each user reduced the number of users who could access the computer at any one time by 30%. Were we to continue this detailed monitoring indefinitely, it would require the purchase of additional equipment to restore services to the previous levels. Needless to say, the costs in terms of denied access and

lost personnel time due to this incident have been considerable.

In retrospect, it appears that the individual(s) who penetrated the Drake academic computer system had no desire to modify or permanently damage either the security of the computer system or any of the information stored in it. However, once the security of the system had been compromised, the "hackers" could return to search for targets of opportunity. Or worse, the "hackers" could return to deliberately erase or modify the programs which control the computer system or to erase or modify any or all of the information which is stored within it. That is, in a single session, the "hackers" could negate the labors of any of the 2900 authorized users of the system.

The incident at Drake University is probably not important in its uniqueness nor are the circumstances which provoked the intrusion particularly at issue. The point to be emphasized here is that this unintended and unauthorized use of the Drake computer acted to deny access to the facility to authorized users and the University was, because of the intrusion, forced to expend time, energy and funds to restore what was viewed as reasonable security to those users. A university community is based on trust. When that trust is violated, there is damage done to that community, damage that limits the ability of the community to accomplish its mission. Due to the threat of penetration by persons external to the university, Drake University faces the need to increase security to the extent of

incurring both additional costs and loss of service to its constituents. The costs are real, both in monetary and in programmatic terms. And as I have indicated before, actually achieving the goal of increased security may in no way be viewed as certain.

With this view in mind, it is instructive to note that penetrating an academic computing system is not particularly difficult for a skilled and determined hacker. By analogy, neither is stealing or damaging a book in a library. Books are placed in a library with the idea that those who need them will use them and return them for future use and that they will be returned in a condition that will make that future use possible. Reasonable security measures are taken to insure that books borrowed will be returned and copying equipment is made accessible so that the temptation to remove pages is reduced. Still, books are stolen and books are mutilated. In a similar vein, ready access to academic computing facilities is deliberate. Programs are designed to encourage and facilitate computer usage and only reasonable and affordable security measures are taken to ensure privacy and appropriate usage. When the conventions of trust are violated in use of the computer system, as is the case with the library, the members of the university community are those who suffer loss. The analogy breaks down when issues of potential extent and impact of computer damage are introduced.

Public awareness of the potential for computer abuse by unauthorized individuals has only recently been heightened. There was, for example, the movie "War Games." Many smile at the antics of the newspaper comic strip character in "Boone County," and the Washington Post carried a story entitled "Teen Computer Break-Ins: High-Tech Rite of Passage." Peter Denning observed that "In their fascination with the 'whiz kids', many media writers avoid the fundamental question: Is breaking into a computer system wrong?" When it was determined that hackers had tampered with the Sloan-Kettering Cancer Institute computer, many began to realize that there were serious implications and that people's lives may be at stake.

While it is difficult to argue that the intrusion into the Drake computer system put lives at stake, it does have serious implications for the students, the faculty, and the administration of the institution. Clearly, then, it is the task of university administrations to provide adequate measures to protect the security of the systems from inappropriate use by those who have legitimate access to the computer. We can and must accept and assume the responsibility of internal discipline and we must in addition be willing and able to prosecute those who engage in fraudulent activities. We cannot, however, given the academic environment of trust, totally protect ourselves from outside intrusion. Legislation is needed to define inappropriate and unauthorized use of computer systems as a punishable crime.

While the events of January 31 were both costly and annoying to us, they may also be taken as instructive. Based on the following quotes, which were made by the individual who helped to arrange the computer penetration, it seems certain that without extraordinary security precautions and the availability of laws that permit prosecution, we will not be able to maintain that essential element of trust that is so critical to an academic computing environment.

> "Our agreement [with the hackers] was that we wanted to prove that we could get in, and stop there. But after spending the night with these guys, I knew they weren't going to walk away from it... I had a lot of people tell me hackers are amoral. I didn't believe it until I saw these guys in action.... They were very arrogant. And they said all they wanted to do was work with computers. ...I'm not sure that I'd call it an addiction, but it was a fetish...."

There is a need for computer crime legislation on both the state and national level. A number of states have responded to the threat to the functioning of higher education and to other societal institutions by enacting computer crime legislation which defines a variety of levels of computer theft and damage and prescribes penalties for offenders. In the State of Iowa, for example, such legislation is currently under consideration. Had this legislation been in force at the time of the penetration of the Drake University computer, and had appropriate public information activities occured, criminal prosecution of the perpetrators could have been pursued and perhaps knowledge of the existence of the law would have operated as a deterrent.

These comments emphasize an incident which occured within a state. There are other processes operating in higher education embracing factors which require federal attention. I have emphasized the need for secure computing services to support the mission of Drake University. A portion of these services is delivered by computing systems at universities in other states via computer networks. The existence of computer networks which cross state boundaries, and which are vital to the operation of institutions of higher education, indicates that the federal government must also respond to the problem. The "interconnectedness" of institutions of higher education is essential to their proper functioning. It is difficult for officials of an individual state to pursue the perpetrators of computer crimes which may actually be committed in another state through use of an interstate network.

Federal response to the problem will have an important secondary benefit. By focusing public attention on the problem, the people of the United States can be educated regarding the seriousness of these issues. This will in turn lead to the recognition that "hacking" is not simply a phenomenon like "streaking," but is, in fact, a practice which seriously impedes the effective functioning of societal institutions.

Public and legislative awareness of the problems posed by security breaches of computer systems due to hackers and other individuals is growing. As we enter the "Information Age," societal institutions have grown increasingly dependent on the availability of secure computing services. If we continue to treat computer crime as intellectual pranksterism, we threaten the effective functioning of these institutions.